

HISTORY

Following the disposition of a Pre Appeal Brief Review requested by Applicant, the claims were again examined by the Examiner. As a result of further examination, claims 1-6, 8-12, 14, 16-23, 25-28, 30-24, 36 and 28-44 stood rejected (non-final) under 35 U.S.C. §102(e) as being anticipated by Abrahams (US patent 6,944,773); and claims 7, 15, 29 and 37 stood rejected (non-final) under 35 U.S.C. §103(a) as being unpatentable over Abrahams in view of Price-Francis (US patent 5,815,252). Applicant responded on December 7, 2006.

In a Final office action dated 3/06/07, claims 4 and 44 are objected to, claims 1-6, 8-12, 14, 16, 17-21, 23, 25-28, 30-34, 36 and 38-43 stand rejected to under 35 U.S.C. §102(e) as being anticipated by Lewis (US Patent 6,213,391), and claims 7, 15, 29 and 37 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Lewis in view of Price-Francis (US Patent 5,815,252), and claims 22 and 44 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Lewis in view of Abrahams (US Patent 6,944,773).

Applicant has amended claims 1, 3, 7, 11, 22,23 and 44, canceled claim 6, and submits the following remarks in response to the rejection.

REMARKS

What is needed in the biometric field are more secure means to authenticate users and provide access to authenticated users. System that can help facilitate expedited user authentication where biometric information is stored remotely are also needed. Prompt user identification can be facilitated with wireless features of the present invention. Wireless identification of a user by an electronic system can facilitate retrieval of user profiles including biometric attributes from remote servers by an electronic system that are needed for user authentication. A retrieved user's profile is then used for the electronic system to determine user authentication by comparing biometric attributes randomly requested from a user using a biometric user interface to biometric attributes associated with the user profile retrieved from the remote server.

In response to the rejections and objection of record, Applicant has amended independent claims 1, 22, 23 and 44. Neither Lewis, Abrahams or Price-Francis, alone or in combination with each other, teach or suggest:

- (Independent Claim 1) - a method for biometrically securing access, said method comprising the steps of: wirelessly obtaining identification of a user with an electronic system using a contactless card reader in communication with said electronic system, the identification of said user further retrieved from a contactless smart card after said contactless smart card establishes a contactless link to support wireless communication between said contactless smart card and said contactless card reader; accessing a user profile including biometric attributes associated with said user through a computer network from a remote server based on the identification of said user obtained wirelessly from said contactless smart card; prompting said user to input to a biometric user interface associated with said electronic system at least one biometric attribute randomly selected from said user profile retrieved from said remote server; and said electronic system permitting said user access to perform a user-desired activity if at least one biometric attribute input by said user to said biometric user interface associated with said electronic system matches said at least one biometric attribute randomly selected from said user profile; or

- (Independent Claim 22) - a method for biometrically securing access to a secure area, said method comprising the steps of: wirelessly obtaining identification of a user by an electronic system using a contactless card reader in communication with said electronic system, the identification of said user further retrieved from a contactless smart card after said contactless smart card establishes a contactless link with said contactless card reader that supports wireless communication between said contactless smart card and said contactless card reader; based on said wirelessly obtained identification, said electronic system using a computer network to obtain a user profile associated with said user from a remote server said user profile including biometric attributes; said electronic system prompting said user to input into a biometric user interface associated with said electronic system at least one biometric attribute randomly selected by said electronic system from said user profile retrieved from said remote server; and permitting said user to access a secure area if said at least one biometric attribute

input by said user to said biometric user interface match biometric attributes included in said user profile in an order that said at least one biometric attribute is requested by said electronic system; or

- (Independent Claim 23) – a system for biometrically securing access, said system comprising: an electronic system adapted to permit a user to perform a user-desired activity if at least one biometric attribute input by the user to said biometric user interface matches said at least one biometric attribute randomly selected from a user profile accessible by the electronic system from a remote server based on identification of a user obtained wirelessly from a contactless smart card in wireless communication with a contactless card reader associated with the electronic system; a contactless smart card reader associated with said electronic system; and a biometric user interface associated with said electronic system adapted to enable said user to input at least one biometric to said electronic system for comparison to at least one biometric attribute randomly selected by said electronic system from said user profile; wherein said electronic system is adapted to permit said user to perform a user-desired activity if at least one biometric attribute input by said user to said biometric user interface matches said at least one biometric attribute randomly selected from said user profile by said electronic system; or

- (Independent Claim 44) – a system for biometrically securing access to a secure area, said system comprising: an electronic system including a contactless smart card reader, a biometric interface and access over a computer network to a remote server, said electronic system adapted to permit a user to access a secure area if at least one biometric attribute input by the user to said biometric user interface matches at least one biometric attribute randomly selected by said electronic system from a user profile accessible by the electronic system over said computer network from said remote server, said remote server adapted to store at least one user profile including biometric attributes and provide said electronic system access to said at least one user profile and said electronic system further adapted to wireless retrieve user identification from a contactless smart card through said contactless smart card reader after a wireless communication link is established between said contactless smart card reader and a contactless smart card held by the user.

Support for the amendments to independent claims 1, 22, 23 and 44 can be found within the disclosure as originally filed, and in particular in pages 27-29 where particular reference is made to "smart cards", the Abstract, and Figure 1 (see reference numeral #20, smart card used at ATM). . No new matter has been added with the current amendments.

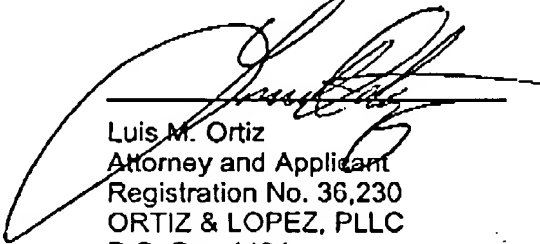
CONCLUSION

Applicant believes the amendment overcomes the rejections and request reconsideration of the pending claims, 1-5, 7-12, 14-23, 25-34 and 36-44.

Respectfully submitted,

Dated: July 6, 2006

Tel. (505) 314-1311
Fax. (505) 314-1307



Luis M. Ortiz
Attorney and Applicant
Registration No. 36,230
ORTIZ & LOPEZ, PLLC
P.O. Box 4484
Albuquerque, NM 87196-4484